

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of

Framework for Next Generation 911 Deployment

PS Docket No. 10-255

Via the ECFS

COMMENTS OF IEEE 802.18

IEEE 802.18, the Radio Regulatory Technical Advisory Group (“the RR-TAG”) within IEEE 802¹ hereby submits its Comments in the above-captioned Proceeding. This document was prepared and approved by the RR-TAG, and also was reviewed by the IEEE 802 Executive Committee.²

The members of the RR-TAG that participate in the IEEE 802 standards process are interested parties in this proceeding. We appreciate the opportunity to provide these comments to the Commission.

INTRODUCTION

1. On December 21, 2010, the Commission released document FCC 10-200, a Notice of Inquiry (“NOI”) titled “Framework for Next Generation 911 Deployment”.
2. In our response, the RR-TAG has incorporated inputs from subject matter experts within IEEE 802, specifically from the IEEE 802.23 Emergency Services Working Group (“802.23”) and from other interested parties within IEEE 802.
3. 802.23 is drafting a new standard which defines a media independent framework within IEEE 802 to provide consistent access and data that facilitate compliance to applicable civil authority requirements for communications systems that include IEEE 802 networks. This includes a data link layer interface for a consistent view of IEEE 802 networks by IP (Internet Protocol) based citizen-to-

¹ The IEEE Local and Metropolitan Area Networks Standards Committee (“IEEE 802” or the “LMSC”)

² This document represents the views of IEEE 802.18. It does not necessarily represent the views of the IEEE as a whole or the IEEE Standards Association as a whole.

authority emergency services capabilities from the Internet Engineering Task Force (IETF)

Emergency Context Resolution with Internet Technologies (ECRIT). This standard specifies a Layer 2 entity and associated behaviors with a uniform structure of management information for transferring data required by an emergency services request.

4. For more overview information on the 802.23 standard, please refer to the Working Group website at www.ieee802.org/23/.
5. The members of the RR-TAG and of 802.23 appreciate this opportunity to provide inputs to the Commission's NG911.
6. In order to make our responses consistent with the NOI, we will refer to the paragraph and question we are responding to in the following paragraphs.

PARAGRAPH 16, 17: INTERCONNECTED VOIP E911

7. The method described does not provide a realistic view of the mobility of VoIP devices. The mobility of current VoIP platforms (e.g., Wi-Fi handsets) is such that movement can often be constant, including movement between access providers. Any approach which is dependent upon any sort of entry from the subscriber will not be sufficient. VoIP Service Providers have no de-facto access to location information.
8. The difficulty with the Commission's rule as currently written is that the VoIP service provider has no assurance that it has access to: (1) a conventional call back number, or (2) accurate location information nor that the "Registered Location" will be of any actual value to the PSAP.
9. Given the layer separation (modeled after the OSI 7-layer model) and architecture of VoIP systems, the required information does not originate at the service level.
10. We believe that further standardized mechanisms need to be added at layers below the service provider level for this information and that protocols need to be standardized to make this information available to the service provider in order to adequately fulfill this mandate.

PARAGRAPH 49: TRANSPORT MECHANISMS IN AN NG911 ENVIRONMENT

11. IEEE 802.23 is investigating the technical feasibility of adding a special facility only for real time IP Emergency Service (e.g. VoIP). Such service would be configured (1) so that it may be available to unauthorized users at either or both Layer 2 and the service layer and (2) goes around any VPN/tunneling mechanism which may obscure the true network location of the specific L1/L2 network.
12. Extending such service availability to non real-time applications such as e-mail might be quite difficult and would certainly make the security considerations (e.g. protection against false use) of

the special facilitation more difficult to deal with. It might be better from a lower layer networking point of view to have non real-time traffic use normal 802 network services.

13. We believe that IEEE 802 is an appropriate forum to develop open standards for L1/L2 Emergency Services solutions that would apply to IEEE 802 or equivalent packet based digital networks.

PARAGRAPH 52: NG911 CAPABLE DEVICES

14. Rather than a hardware device orientation, we believe that initially the requirement for NG911 capabilities should be attached to devices that have configured functionality able to communicate to the PSTN. The question should move away from hardware devices. Many devices have rich user interfaces, software configurability and Internet connectivity.
15. It is our opinion that requirements for NG911 capabilities should be limited to facilities that are (1) real time in the eyes of the user and (2) We believe that the question should not be "what devices can usefully provide emergency calling services?"

PARAGRAPH 53: E911 SCOPE ORDER AND NG911

16. **Question: Should the Commission consider expanding or modifying the four criteria from the E911 911 Scope Order to apply to additional NG911 participants? For example, should hot-spot providers that are not traditional communications providers, such as coffee shops, hotels, bus lines, and public parks be expected to play a role in the deployment of NG911?**
17. It would be inappropriate and unfortunate if NG911 requirements placed the burden of providing VoIP enabling bandwidth upon anyone who wishes to provide a hot spot for users that might otherwise be limited to (for example) e-mail and web access. It is our feeling that only if a hot-spot provider (1) provides sufficient user bandwidth to support VoIP and (2) has a default VoIP service provider, should they be required to provide NG911 service. We believe that there is sufficient indication space within the IEEE service model to provide an indicator in "hot-spot beacons" to show whether NG911 service would be available to users.

SECTION 3 PARAGRAPH 54: INTEROPERABILITY AND STANDARDS

18. **Questions: We seek comment on how best to ensure such compatibility in the formatting and coding of text, photos, and other digital information. Should there be standards for media encodings?**
19. **Should we specify minimal performance ranges, e.g., minimum file sizes for digital images, that NG911 networks must support and PSAPs be able to accept?**

-
20. We don't believe that minimum file/image sizes will be an issue. We are much more concerned with the impact on network performance and transmission time of large files, especially given the rapid growth rate of image sensor resolution.

PARAGRAPH 55: DIGITAL INFORMATION STANDARDS

21. **Questions: If there is a need to develop standards for digital information transported on NG911 networks, what entity should set and update these standards, or assist in their coordination? Should the standards be national or international?**
22. **Are there standards efforts currently under way that could form the basis for future evolution in this regard? Should specific technical standards or architectures be mandated? How can the interoperability of end user devices and PSAP devices be ensured (e.g., through interoperability testing)?**
23. **Should there be a certification process that indicates whether a device or downloadable software application is compliant with certain standards? If so, what form of certification seems to be the most suitable, e.g., self-certification or approved certification organizations? Should all devices of a certain class be required to meet the certification criteria? As more people, especially within the disability community, begin to make video-based telephone calls, are there steps needed to ensure that NG911 networks interoperate seamlessly with the video software and applications being utilized in smart phones, tablets, computers and other devices? Similarly, are there steps needed to ensure interoperability with the video communication services provided by all video relay service providers?**
24. Given the mobility of users in today's world, we believe that payload (e.g. PDF, MPEG) and transport standards that are accepted worldwide are a must.
25. For transport standards, established industry-led standards development organizations have sufficient scope and cooperative working arrangements to make a set of internationally accepted standards feasible.
26. National and regional government agencies should work together to define requirements in a consistent manner and in such a manner to make internationally compatible systems that have a minimum of configuration differences between jurisdictions.

PARAGRAPH 60: N11 NUMBERS AND OTHER SERVICES FOR EMERGENCY COMMUNICATIONS

27. **Questions: Can such coordination and integration be helpful and cut costs? How will the deployment of NG911 address N11 numbers, including N11 services such as 311, which is designated for non-emergencies? How will the deployment of NG911 impact other emergency**
-

services, such as poison control centers using 800 services? How will the deployment of NG911 affect TRS that use 711?

28. Our answer to the first question is yes. We expect to share most of the infrastructure with only minimal distinction for ES calls.
29. We expect only to have a differentiation between emergency and non-emergency calls. This distinction will not be based on the numeric structure of the N11 PSTN dial string. We expect there to be sufficient address space in the SIP header to address multiple emergency services or sub-types thereof.

PARAGRAPH 63: MLTS FOR EMERGENCY COMMUNICATIONS IN AN NG911 ENVIRONMENT

30. **Questions: In light of NG911's potential impact on MLTS, we seek comment on whether the Commission has the jurisdiction to regulate MLTS operators. How will the deployment of NG911 improve emergency services for MLTS users? Will MLTS operators be able to provide improved location information in an NG911 environment?**
31. We believe properly executed NG911 technology will provide location from the originating location (without regard to PSTN phone number) as opposed to the current system which does a centralized reverse lookup based on ANI.

PARAGRAPH 74: CONFIDENTIALITY AND PRIVACY CONCERNS

32. **Questions: In light of the shared nature of NG911 architecture, we seek comment on whether privacy laws or regulations will need to be modified to adapt to the NG911 environment. What privacy concerns will be introduced with the deployment of NG911? What existing or new regulations might be necessary to ensure appropriate privacy controls? Will the definition of a "911 call" need to be modified in certain statutes and rules? How should we address concerns regarding private personal information that may be transmitted as part of an NG911 communication, for example, personal medical information that NG911 can provide to PSAPs and other third parties? How can 911 call takers at virtual PSAPs legally access 911 call data when necessary, while requiring adherence to appropriate confidentiality, disclosure, and retention statutes and rules?**
33. It is the belief of IEEE 802 that most of the privacy concerns voiced here are outside the scope of the L1/L2 network. For 911 calls placed through a "call based mechanism", we believe that the normal security associated with a normal telephone call is sufficient security in the L1/L2 network until we are in possession of regulations that declare otherwise. L1/L2 networks do not normally do any more than transient storage of the payload data stream. There is normally some information saved for a

short period of time regarding the logical state of the network that may need to be expanded to support expected NG911 requirements for callback. Regulations should be explicit about security requirements for the data associated with this saved state information.

PARAGRAPH 76: LOCATION CAPABILITIES

34. **Questions: To what degree should federal regulations require that access providers provide call location data to end systems and/or voice service providers on reasonable and non-discriminatory terms, using standard protocol interfaces? How can stationary, nomadic, and mobile end systems in wireline and non-cellular wireless networks (including Wi-Fi) reliably discover their location information to ensure call routing and dispatch? What, if any, obligations need to be imposed on Internet service providers, residential and enterprise equipment vendors, and other parties to ensure that location information can be discovered, conveyed, and validated? Is there a need for a national or regional certification entity that will allow a provider of location information to cryptographically sign the location information?**
35. Adding facilities in the IEEE 802 infrastructure to provide location information to end systems may add significant expense and complexity to the current architecture and implementations. However, we do believe that IEEE 802 has come up with technical approaches which can provide location to a higher degree of accuracy than a router only based system. Specific requirements as to authentication and validation would facilitate standards in this area.
36. There certainly are cryptographic standards in this area that could provide such a service. We take no position as to whether a requirement is needed. If there is such a requirement then it would be helpful to use existing 802 standards.

PARAGRAPH 80: UNAUTHORIZED ACCESS

37. **Questions: We seek comment on whether such emergency-call-only credentials would be desirable and feasible? If so, how can they be implemented? What regulatory arrangements would be necessary to facilitate this emergency-call authentication?**
38. The layered architecture of IP networks, which tends to produce networks where several unrelated vendors are often involved in any "call", complicates this issue significantly. Access to services at each level of the system is a separate issue and requires analysis for each combination thereof. IEEE 802.23 intends to publish an analysis of this situation and what it believes is the real result of each combination.

PARAGRAPH 81: AUTHORIZATION PROCEDURES

39. **Questions: We seek comment on how this problem can be addressed. When would it be appropriate for the NG911 system to support emergency calls without authentication and/or authorization? Should ASPs be required to support emergency calls for zero-balance customers? Should providers of public and semipublic wireless data networks, such as 802.11 hot spots, be required to provide access for emergency calls?**
40. This is largely a policy question that we believe will be heavily influenced for VoIP by the lessons learned from equivalent rules in the cellular market. 802.11 hot spots do not necessarily have the bandwidth or services to support emergency calls. Adding a requirement to support emergency calls might well be a large enough burden that it would significantly reduce the availability of such hot spots.

CONCLUSION

41. IEEE 802.18 appreciates this opportunity to provide feedback with respect to the Commission's NG911 NOI.

Respectfully submitted,

/s/
Michael Lynch
Chair, IEEE 802.18 Radio Regulatory TAG
108 Brentwood Court
Allen, TX 75013
(972) 814-4901
freqmgr@ieee.org